On the weight adjacency matrix of convolutional codes

Schneider, Hans-Gert

Publication date:
2008

6 On Concepts of Equivalence for Convolutional Codes

In Chapter 2 two different notions of isometry for block codes have been introduced which happen to coincide due to Theorem 2.8. It is widely accepted that these are meaningful concepts and therefore they are well established in the literature. A reason for this is that they really describe when two codes are equivalent, which translates to being "'equally good"'. For convolutional codes it has not yet been clarified, when two codes perform "'equally well"'. One reason is, that it is unclear how many properties of the codes should be taken into account.

Of course, one could call two codes equivalent, if they are isometric; that is, if there is a $\mathbb{F}[z]$-linear weight-preserving bijection between them. Taking $\mathbb{F} = \mathbb{F}_2$ it is straightforward to check that the codes im $\begin{pmatrix} 1 & z \end{pmatrix}$ and im $\begin{pmatrix} 1 & 1 \end{pmatrix}$ are in fact isometric. Necessarily they have the same minimum distance, but the complexity, which is an important parameter, when comparing the performance of two codes, is different. This is reflected in the generalised Singleton-bound as given in Proposition 5.12. As far as this bound is concerned the code with the constant encoder matrix is clearly superior. Hence one would not like to identify these two isometric codes to be equivalent. The toy example and the generalised Singleton-bound suggest, that the complexity is an important parameter as well and equivalent codes should share this invariant.

Due to the fact that equivalent block codes are isometric they share the same weight enumerator. In the toy example given above, the two isometric convolutional codes do not have the same WAM. Even worse, the different complexities result in the WAMs of the two codes not even having the same size. The latter can of course easily be fixed by demanding that the codes should have the same complexity in addition of being isometric. Two convolutional codes of complexity 1 that are isometric are given by the minimal encoders $\begin{pmatrix} 1 & 1+z \end{pmatrix}$ and $\begin{pmatrix} z & z+1 \end{pmatrix}$. The second code is easily identified to be the reversal code of the first one. As the WAM of the reversal code can be obtained by the WAM of the original code via transposition according to Corollary 3.16, the two codes share the same weight adjacency matrix if their WAM is symmetric. It is easy to calculate that the WAM of the first encoder is $\begin{pmatrix} 1 & W^2 \\ W & W \end{pmatrix}$. So they do not share the same WAM. Again, from an applications point of view both codes are indeed not equivalent as their column distances are different (see [15] p.110). This shows that even an isometry which preserves the complexity of the codes does not leave all parameters invariant, that are important for the code's performance.

As the WAM contains most, if not all, parameters that are important for the performance of a convolutional code, it is an interesting approach to see in which way two codes that share the same WAM are connected. For block codes there is no strong connection. If two codes have the same weight enumerator they need not be isometric, but there is only a weight-preserving bijection between them. This is illustrated in the following example taken from [14], example 1.6.1.

Example 6.1 Let $\mathbb{F} = \mathbb{F}_2$ and consider the codes

$$\mathcal{C}_1 := \operatorname{im} G_1 = \operatorname{im} \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \text{ and } \mathcal{C}_2 := \operatorname{im} G_2 = \operatorname{im} \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

One computes the weight enumerator of both codes to be $1 + 3W^2 + 3W^4 + W^6$, but they are not isometric. This can quickly be verified by exploiting that the first code is self-orthogonal, which implies $G_1 G_1^t = 0$. But the second is not, as the first and second row of the encoder are not orthogonal to each other. If the codes were isometric, the MacWilliams Extension Theorem (Theorem 2.8) would imply there is a permutation matrix $P \in \mathrm{GL}_6(\mathbb{F})$ and a $U \in \mathrm{GL}_3(\mathbb{F})$ such that $G_2 = UG_1P$. But then $0 \neq G_2 G_2^t = UG_1P(UG_1P)^t = UG_1PP^tG_1^tU^t = 0$, and so the codes are not isometric.

Surprisingly, for a special class of convolutional codes a much stronger result may be derived. To do so I have to recall the concept of monomial equivalence. Recall, that two block codes of length n are monomially equivalent if there is a permutation matrix $P \in \mathbb{F}^{n\times n}$ and an invertible diagonal matrix $M \in \mathbb{F}^{n\times n}$ such that PM establishes an isomorphism between the codes. This definition may be applied for convolutional codes as well. It may at first sight be surprising that the matrix M is not allowed to have polynomial entries, but this is an implication from the condition that it should be invertible. Moreover, it has already been demonstrated that rescaling by z for example can change important invariants of the codes. The following assertion generalises a well known fact for block codes, is easily verified and may be found in [8].

Proposition 6.2 *If the convolutional codes $\mathcal{C}$ and $\mathcal{C}'$ are monomially equivalent they share the same generalised WAM.*

By virtue of this proposition one easily sees that the concepts of isometry and monomial equivalence do not coincide for convolutional codes, as I have given an example of isometric codes that do not share the same WAM. Hence the classical MacWilliams Extension Theorem 2.8 may not simply be transferred to convolutional codes.

Theorem 6.3 *Let $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}[z]^n$ be two codes and assume that all Forney indices of $\mathcal{C}$ are positive. Then $\mathcal{C}$ and $\mathcal{C}'$ are monomially equivalent if and only if their generalised WAMs coincide.*

To prove this Theorem I need some preparation.

Proposition 6.4 *Let $G, \bar{G} \in \mathbb{F}[z]^{k\times n}$ be minimal encoders and $\deg(G) = \deg(\bar{G}) = \delta$. Let (A, B, C, D) and $(\bar{A}, \bar{B}, \bar{C}, \bar{D})$ be the associated controller canonical forms. Then the following are equivalent:*

(i) $G = W\bar{G}$ *for some* $W \in \mathrm{GL}_k(\mathbb{F}[z])$.

(ii) The systems (A, B, C, D) *and* $(\bar{A}, \bar{B}, \bar{C}, \bar{D})$ *are equivalent under the full state feedback group, that is, there exist matrices* $T \in \mathrm{GL}_\delta(\mathbb{F})$, $U \in \mathrm{GL}_k(\mathbb{F})$, $M \in \mathbb{F}^{\delta\times k}$ *such that*

$$\bar{A} = T^{-1}(A - MB)T, \bar{B} = UBT, \bar{C} = T^{-1}(C - MD), \bar{D} = UD \tag{6.1}$$

PROOF: (ii) $\Rightarrow$ (i): Define the $k \times k$-matrix $V := I + B(z^{-1}I - A)^{-1}M$. From systems theory it is well known [2, p. 346, Eq. (2.43)] that

$$B(z^{-1}I - A)^{-1}C + D = VU^{-1}\big(UB(z^{-1}I - A + MB)^{-1}(C - MD) + UD\big), \tag{6.2}$$

thus $G = VU^{-1}\bar{G}$. Due to nilpotency of A the matrix V is polynomial. But then $W := VU^{-1}$ is even unimodular since G and $\bar{G}$ are both basic. This yields (i).
(i) $\Rightarrow$ (ii): First notice that equivalence under the full state feedback group is indeed an equivalence relation. Assumption (i) implies that G and $\bar{G}$ have the same row degrees. Since reordering of the rows of G retains the specific requirements of the controller canonical form I may further assume that G and $\bar{G}$ both have row degrees $\nu_1 \geq \ldots \geq \nu_k$. Then $A = \bar{A}$ and $B = \bar{B}$ since they are both fully determined by the row degrees. Due to reducedness of G and $\bar{G}$ the ith row of W has degree at most ν_i for $i = 1, \ldots, k$, see [5, Main Thm. (4)]. I will show now that

$$W = \big(I + B(z^{-1}I - A)^{-1}M\big)U^{-1} \text{ for some } M \in \mathbb{F}^{\delta\times k},\ U \in GL_k(\mathbb{F}). \tag{6.3}$$

I certainly have to put $U := W(0)^{-1}$ and need to find M such that $B(z^{-1}I - A)^{-1}M = WU - I$. The latter matrix is of the form $WU - I = \Big(\sum_{j=1}^{\nu_i} a_{ij}z^j\Big)_{i=1,\ldots,k}$ for suitable $a_{ij} \in \mathbb{F}^k$. Using that $B(z^{-1}I - A)^{-1} = \mathrm{diag}\big(\begin{pmatrix} z & z^2 & \cdots & z^{\nu_i}\end{pmatrix}\big)_{i=1,\ldots,k} \in \mathbb{F}[z]^{k\times\delta}$, one sees that the matrix $M = (M_1, \ldots, M_k)^t$ where $M_i = (a_{i1}^t, \ldots, a_{i\nu_i}^t)$, satisfies (6.3). Notice that if $\nu_i = 0$ the result is true as well, since in that case the ith block of M is missing and a zero row appears in $WU - I$ and $B(z^{-1}I - A)^{-1}$. Now I have the identity $G = VU^{-1}\bar{G}$ where, again, $V = I + B(z^{-1}I - A)^{-1}M$. Using (6.2) this reads as

$$UB(z^{-1}I - A + MB)^{-1}(C - MD) + UD = B(z^{-1}I - A)^{-1}\bar{C} + \bar{D} = \bar{G}(z). \tag{6.4}$$

Hence $(A - MB, UB, C - MD, UD)$ is a minimal realisation of $\bar{G}$ of complexity $\deg(\bar{G})$. As a consequence, (6.4) implies that the realisations $(A - MB, UB, C - MD, UD)$ and $(A, B, \bar{C}, \bar{D})$ are similar, and this yields (ii). $\square$

Now I can give the proof of Theorem 6.3.

PROOF: The only-if part is in Proposition 6.2. Thus let me assume that $\{\Lambda(\mathcal{C})\} = \{\Lambda(\mathcal{C}')\}$. The outline of the proof is as follows. I will consider the controller canonical forms of the two codes and show that the identity $\{\Lambda(\mathcal{C})\} = \{\Lambda(\mathcal{C}')\}$ implies that these realisations are equivalent under the full state feedback group followed by reordering and rescaling of the output coordinates. With the aid of Proposition 6.4

I can then conclude that the two associated encoder matrices satisfy an identity of the form $G' = WGPR$ for some unimodular matrix W and permutation and rescaling matrices P, R. This implies that the codes are monomially equivalent. I proceed in several steps.

1) I first study the algebraic parameters of the codes and fix suitable realisations. Since the adjacency matrices have the same size, the two codes have the same degree, say δ. Let G, G' be any minimal encoder matrices of $\mathcal{C}$ and $\mathcal{C}'$ and (A, B, C, D) and (A', B', C', D') be the corresponding controller canonical forms, respectively. Then the two systems have complexity δ and they form minimal realisations of the codes $\mathcal{C}$ and $\mathcal{C}'$. Let Λ and Λ' be the associated weight adjacency matrices. By assumption there exist some $T \in GL_\delta(\mathbb{F})$ such that

$$\Lambda'_{X,Y} = \Lambda_{XT,YT} \text{ for all } (X, Y) \in \mathbb{F}^{2\delta}. \tag{6.5}$$

In [8, Thm. 5.1] is has been proven that codes satisfying (6.5) have the same dimension and the same Forney indices. Thus let $k := \dim(\mathcal{C}) = \dim(\mathcal{C}')$. I may assume that both codes have their Forney indices, which are by assumption positive, in the same ordering. Let me denote them by $\nu_1 \geq \ldots \geq \nu_k \geq 1$. Recall that $\delta = \sum_{i=1}^{k} \nu_i$. Now the controller canonical form implies $A' = A$ and $B' = B$.

2) Next I will show that

$$A = T(A - MB)T^{-1} \text{ and } B = UBT^{-1} \text{ for some matrices } M \in \mathbb{F}^{\delta \times k},\, U \in GL_k(\mathbb{F}). \tag{6.6}$$

By definition of the weight adjacency matrix it is for any $(X, Y) \in \mathcal{F}$

$$Y - XA \in \operatorname{im} B \iff \Lambda'_{X,Y} \neq 0 \iff \Lambda_{XT,YT} \neq 0 \iff YT - XTA \in \operatorname{im} B.$$

Putting $\tilde{A} = TAT^{-1}$, $\tilde{B} = BT^{-1}$, I thus get

$$Y - XA \in \operatorname{im} B \iff Y - X\tilde{A} \in \operatorname{im} \tilde{B}.$$

Using $X = 0$ this implies $\operatorname{im} \tilde{B} = \operatorname{im} B$ and hence $BT^{-1} = \tilde{U}B$ for some $\tilde{U} \in GL_k(\mathbb{F})$. On the other hand, for each $X \in \mathbb{F}^\delta$ there exists $u \in \mathbb{F}^k$ and $Y \in \mathbb{F}^\delta$ such that $Y - XA = uB$, hence there exists $\tilde{u} \in \mathbb{F}^k$ such that $Y - X\tilde{A} = \tilde{u}B$. This implies $X(\tilde{A} - A) = (u - \tilde{u})B$. Using for X all standard basis vectors I obtain the identity $\tilde{A} = A + \tilde{M}B$ for some matrix $\tilde{M} \in \mathbb{F}^{\delta \times k}$. Hence I arrive at $A = T^{-1}(A + \tilde{M}B)T$ and $B = \tilde{U}BT$. This in turn yields (6.6).

3) In this step I will prove that (A, B, C', D') and (A, B, C, D) are related via the full state feedback group followed by reordering and rescaling of the output coordinates, see (6.8) below. In order to do so I will compare the entries of the weight adjacency matrices. Consider the minimal realisation $(\bar{A}, \bar{B}, \bar{C}, \bar{D}) = (TAT^{-1}, BT^{-1}, TC, D)$ of the code $\mathcal{C}$. It is easy to see [8, Rem. 3.6] that the associated weight adjacency matrix $\bar{\Lambda}$ satisfies $\bar{\Lambda}_{X,Y} = \Lambda_{XT,YT}$ for all $(X, Y) \in \mathcal{F}$ and hence Equation (6.5) implies

$$\bar{\Lambda} = \Lambda'.$$

Now I can study the entries of these weight adjacency matrices. Since all Forney indices are positive, the matrix B has full rank k. As a consequence, for each pair of states $(X,Y)\in\mathcal{F}$ the set $\{XC'+uD' \mid u\in\mathbb{F}^k : Y=XA+uB\}$ has at most one element. Recalling the definition of the weight adjacency matrix in Definition 3.1 one obtains that the nonzero entries are given by

$$\Lambda'_{X,XA+uB}=\bar{\Lambda}_{X,XA+uB} \text{ for all } (X,u)\in\mathbb{F}^\delta\times\mathbb{F}^k, \tag{6.7}$$

and these entries have the value $\Lambda'_{X,XA+uB}=W^a$ where $a=\mathrm{wt}(XC'+uD')$. On the other hand notice that, due to (6.6), for any $(X,u)\in\mathbb{F}^\delta\times\mathbb{F}^k$ I have

$$XA+uB=X(TAT^{-1}-TMBT^{-1})+uUBT^{-1}=X\bar{A}+\bar{u}\bar{B} \text{ where } \bar{u}=uU-XTM.$$

Thus Definition 3.1 yields $\bar{\Lambda}_{X,XA+uB}=\bar{\Lambda}_{X,X\bar{A}+\bar{u}\bar{B}}=W^b$ where $b=\mathrm{wt}(X\bar{C}+\bar{u}\bar{D})$. As a consequence, (6.7) implies

$$\mathrm{wt}\Big((X,u)\begin{pmatrix}C'\\D'\end{pmatrix}\Big)=\mathrm{wt}\big(X\bar{C}+(uU-XTM)\bar{D}\big)=\mathrm{wt}\Big((X,u)\begin{pmatrix}\bar{C}-TM\bar{D}\\U\bar{D}\end{pmatrix}\Big)$$

for all $(X,u)\in\mathbb{F}^\delta\times\mathbb{F}^k$. Now [8, Lemma 5.4], which is basically MacWilliams' Equivalence Theorem for block codes, yields the existence of a permutation matrix $P\in GL_n(\mathbb{F})$ and a nonsingular diagonal matrix $R\in GL_n(\mathbb{F})$ such that

$$\begin{pmatrix}C'\\D'\end{pmatrix}=\begin{pmatrix}\bar{C}-TM\bar{D}\\U\bar{D}\end{pmatrix}PR.$$

With the help of (6.6) one sees that the realisation (A,B,C',D') of $\mathcal{C}'$ is of the form

$$\left.\begin{aligned}(A,B,C',D') &= (T(A-MB)T^{-1},UBT^{-1},(\bar{C}-TM\bar{D})PR,U\bar{D}PR)\\ &= (T(A-MB)T^{-1},UBT^{-1},T(C-MD)PR,UDPR).\end{aligned}\right\} \tag{6.8}$$

4) Now I can apply Proposition 6.4 and obtain for the associated encoder matrices

$$G'=WGPR \text{ for some } W\in GL_k(\mathbb{F}[z]).$$

Thus $\mathcal{C}=\operatorname{im}G$ and $\mathcal{C}'=\operatorname{im}G'$ are monomially equivalent. This completes the proof. □

Although this result is restricted to a seemingly small class of convolutional codes, it covers the codes that are of greatest interest for applications. Any code not in this class has constant codewords. The minimal distance of a code with constant codewords is less than or equal to the minimal distance of the block code it contains. Hence its minimal distance cannot be better than that of this block code, which makes the codes not particularly suitable for applications.

The result may not be generalised further. Example 6.1 already shows that it does not hold for block codes in general. Moreover, one can construct a convolutional code with constant codewords for which it is wrong using the two block codes from the Example.

Example 6.5 Using the rows of the encoders of Example 6.1 in a suitable way one obtains

$$G = \begin{pmatrix} 1 & 1 & z & z & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad \bar{G} = \begin{pmatrix} z+1 & 1 & z & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2[z]^{2\times 6}.$$

Both matrices are minimal. The WAM of the associated controller canonical forms are both given by

$$\Lambda = \begin{pmatrix} 1+W^6 & W^2+W^4 \\ W^2+W^4 & W^2+W^4 \end{pmatrix}.$$

But the codes $\mathcal{C} = \operatorname{im} G$ and $\bar{\mathcal{C}} = \operatorname{im} \bar{G}$ are not monomially equivalent. This can be seen by computing UG for all $U \in GL_2(\mathbb{F}_2[z])$ such that UG is reduced with indices 1 and 0 again. The only options are

$$U \in \left\{ I_2, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1+z \\ 0 & 1 \end{pmatrix} \right\}$$

and it is seen by inspection that in none of these cases UG has, up to ordering, the same columns as $\bar{G}$ (over $\mathbb{F}_2$ one can disregard rescaling matrices). It is, however, not clear whether the codes are isometric.

It remains open, if there is a similarily tight connection between monomial equivalence and a suitable notion of isometry as in the block code case. Moreover, it is totally open whether such a notion of isometry is meaningful for practical considerations of convolutional codes.